PATENT ABSTRACTS OF JAPAN

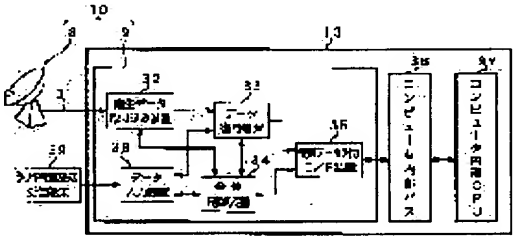
(11)Publication number : 11-308582
(43)Date of publication of application : 05.11.1999

(51)Int.CI. H04N 7/08
H04N 7/081
H04H 1/00
H04L 9/14
H04N 7/167

(21)Application number : 10-115451 (71)Applicant : SONY CORP
(22)Date of filing : 24.04.1998 (72)Inventor : ISHII MAKOTO

(54) DATA RECEIVER, ITS METHOD AND DATA TRANSMISSION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data receiver by which only a prescribed person can receiver data of a large capacity and many kinds of data simultaneously in the data transmission system where data with a large capacity are transferred through many channels and that utilizes a communication satellite.
SOLUTION: The data receiver 10 is provided with a reception antenna and a coaxial cable 31 that receive signal data distributed via a communication satellite, a satellite data acquisition device 32 that descrambles the signal data depending on the scrambling applied to the data and extracts a digital signal, a data decoder 33 having a data acquisition function that extracts prescribed data from the digital signal, a decoding function that decodes the digital data acquired by the data acquisition function by using an encryption key, and having a decoding key management function to manage the decoding key, and a received data output I/F device 35 that outputs the data decoded by the data decoder 33 externally.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－308582

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｎ	7/08		Ｈ０４Ｎ	7/08	Ｚ
	7/081		Ｈ０４Ｈ	1/00	Ｆ
Ｈ０４Ｈ	1/00		Ｈ０４Ｌ	9/00	６４１
Ｈ０４Ｌ	9/14		Ｈ０４Ｎ	7/167	Ｚ
Ｈ０４Ｎ	7/167				

審査請求　未請求　請求項の数16　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－115451

(22)出願日　平成10年(1998)４月24日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　石井　眞
東京都品川区北品川６丁目７番35号　ソニー株式会社内

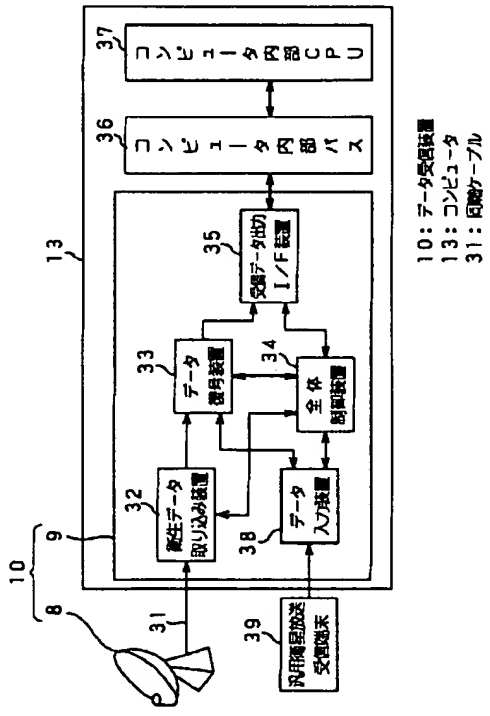
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　データ受信装置及び方法、並びにデータ送信方法

(57)【要約】

【課題】　多チャンネル及び大容量でデータの転送を行通信衛星を利用したデータ伝送システムにおいて、所定の者のみが大容量のデータかつ多種類のデータを同時に受信することを可能にするデータ受信装置の提供を目的とする。

【解決手段】　データ受信装置１０は、通信衛星を介して配信される信号データを受信する受信アンテナ８及び同軸ケーブル３１と、上記信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出す衛星データ取り込み装置３２と、上記ディジタル信号から所定のデータを取り出すデータ取得機能、当該データ取得機能により取得したディジタルデータを暗号鍵により復号する復号機能及び上記復号鍵を管理する復号鍵管理機能を有するデータ復号装置３３と、データ復号装置により復号されたデータを外部に出力する受信データ出力Ｉ／Ｆ装置３５とを備えている。



1

【特許請求の範囲】

【請求項１】　衛星通信路を介して配信される信号データを受信するデータ受信装置において、
上記衛星通信路を介して配信される信号データを受信する受信手段と、
上記信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出すデスクランブル手段と、
上記ディジタル信号から所定のデータを取り出すデータ取得手段と、
上記データ取得手段により取得した暗号化されたデータを暗号鍵により復号する復号手段と、
上記暗号鍵を保管する暗号鍵保管手段と、
上記復号手段により復号されたデータを外部に出力する出力手段とを備えることを特徴とするデータ受信装置。

【請求項２】　上記暗号鍵により復号される上記暗号化されたデータは、映像・音声データとともに伝送されるコンピュータのデータであることを特徴とする請求項１記載のデータ受信装置。

【請求項３】　上記暗号化されたデータは、複数のパケットに分割されて配信さてきたデータであって、
上記復号手段は、実時間で上記各パケット毎に上記暗号化されたデータを復号することを特徴とする請求項２記載のデータ受信装置。

【請求項４】　上記暗号鍵保管手段は、複数の暗号鍵を管理しており、
上記復号手段は、パケット毎に暗号鍵を交換して上記暗号化されたデータを復号することを特徴とする請求項３記載のデータ受信装置。

【請求項５】　上記暗号鍵の選択は、データバスを介して外部から設定されることを特徴とする請求項４記載のデータ受信装置。

【請求項６】　上記データ取得手段、復号手段及び出力手段は、一枚の基板上において構成されてなることを特徴とする請求項１記載のデータ受信装置。

【請求項７】　上記出力手段は、データバスに接続されていることを特徴とする請求項６記載のデータ受信装置。

【請求項８】　上記復号手段は、上記暗号化されたデータの復号に用いる所望の暗号鍵がないときには、当該復号対象としている暗号化されたデータが格納されているパケットを破棄することを特徴とする請求項１記載のデータ受信装置。

【請求項９】　上記復号手段は、当該暗号化されたデータを送信した送信側が保持している暗号鍵と同じ上記暗号鍵保管手段において保管されている上記暗号鍵を用いて復号することを特徴とする請求項８記載のデータ受信装置。

【請求項１０】　上記復号鍵管理手段は、随時変更される可能性があるセッション鍵と、当該復号管理手段により恒久的に管理されているマスター鍵の２種類の鍵を管理することを特徴とする請求項１記載のデータ受信装置。

2

【請求項１１】　上記復号手段は、ユーザからの設定により暗号方式を実時間で変更することが可能とされることを特徴とする請求項１記載のデータ受信装置。

【請求項１２】　上記衛星通信路とは別に、双方向のデータ伝送が可能な双方向データ伝送路を備え、
上記暗号化されたデータは、当該双方向データ伝送路を介して配信元に配信要求したデータからなることを特徴とする請求項１記載のデータ受信装置。

【請求項１３】　上記衛星通信路により伝送される衛星映像音声放送を受信する汎用の衛星映像音声放送用の受信端末を備えていることを特徴とする請求項１記載のデータ受信装置。

【請求項１４】　衛星通信路を介して配信される信号データを受信するデータ受信方法において、
上記衛星通信路を介して配信される信号データを受信する受信工程と、
上記信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出すデスクランブル工程と、
上記ディジタル信号から所定のデータを取り出すデータ取得工程と、
上記データ取得工程により取得した暗号化されたデータを、暗号鍵保管手段に保管されている暗号鍵により復号する復号工程と、
上記復号工程により復号されたデータを外部に出力する出力工程とを有することを特徴とするデータ受信方法。

【請求項１５】　スクランブル処理した映像音声情報を衛星通信路を介して配信するデータ送信装置において、
上記衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加するデータ暗号化工程と、
上記暗号鍵を用いて暗号化されたデータ及び当該暗号化されたデータに付加されている配信先情報に対して、上記映像音声情報をスクランブル処理するのと同一の処理によりスクランブル処理を行うスクランブル処理工程と、
上記スクランブル処理された各種データを上記衛星通信路上に伝送するデータ伝送工程とを有することを特徴とするデータ送信方法。

【請求項１６】　上記暗号鍵を用いて暗号化されたデータ及び当該暗号化されたデータに付加されている配信先情報を複数のパケットに分割してから上記スクランブル処理手段により、スクランブル処理が施されることを特徴とする請求項１５記載のデータ送信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、衛星通信路を利用

してデータの送受信を可能にするデータ受信装置及び方法、並びにデータ送信方法に関する。

【０００２】

【従来の技術】近年、動画像等の圧縮技術により、例えば、現行放送やＨＤＴＶ、ＡＶ機器などにおいて画像等の符号化方式に採用されているＭＰＥＧ２（Moving Picture Experts Group Phase 2）は、従来のアナログ放送に比べてディジタルによる多チャンネル化とチャンネル当たりのコストの削減をもたらしている。そして、このことは、映像・音声のみならずデータ放送等のサービスも可能にするといえる。そして、ＭＰＥＧ２方式による放送は、通信衛星を利用した多チャンネルディジタル放送としても採用されており、益々一般的になりつつある。

【０００３】例えば、上記多チャンネルディジタル放送においては、衛星の高速転送スピード、例えば２７ＭＨｚトランスポンダの場合、最大３０Ｍｂｐｓ、を生かした各種のデータ放送が実施されている。ここで、データ放送には、例えば音楽サービス、ゲームサービス、雑誌情報サービス、インターネット（WWW）サービスなどがある。

【０００４】

【発明が解決しようとする課題】ところで、上述のような通信衛星を用いて配信されるデータを、所定の者、例えば、契約者のみに受信させることが提案されている。このようなデータの配信方法は、例えばデータ提供者が契約者のみにデータを送信したいとき、又は受信側のユーザが固有の情報として配信してもらいたいときなどに採用されると考えられるが、この場合、個人レベルでの秘密保持機構が必ず必要になる。

【０００５】また、個人レベルの秘密を保持してデータを配信する手段として、配信データ暗号化が挙げられるが、通信衛星を利用することを考慮した場合には、最速３０Ｍｂｐｓの高速データ転送とされることから受信側において受信中のデータを、実時間かつ高速に暗号化されたデータを復号しなければならない。

【０００６】さらには、上記秘密保持されているデータが同時刻に複数（例えば、複数種類、複数番組）受信しなければならないような状況も生じると考えられ、このような場合であっても、実時間で復号するような機構が必要となる。

【０００７】なお、上述したように、各種データ放送サービスにより配信されるデータを受信するには、復号機能等の各種機能が要求されると考えられるが、同一のハードウエアで当該要求される処理を行うことが当該要求に耐え、効率よくデータの処理を行い得るデータ受信装置を提供することになるといえる。

【０００８】また、今後サービス開始するであろう様々なデータ放送またはデータ通信サービスに汎用的に対応すること、例えば、現行及び今後の汎用的受信端末（ＩＲＤ；Interactive Reciever Decorder）との接続も容易に行えるようにすることなども重要である。

【０００９】本発明は、上述の実情に鑑みてなされたものであって、多チャンネル及び大容量でデータの転送を行通信衛星を利用したデータ伝送システムにおいて、所定の者のみが大容量のデータかつ多種類のデータを同時に受信することを可能にするデータ受信装置及び方法、並びにデータ送信方法の提供を目的とする。

【００１０】

【課題を解決するための手段】本発明に係るデータ受信装置は、上述の課題を解決するために、衛星通信路を介して配信される信号データを受信する受信手段と、信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出すデスクランブル手段と、ディジタル信号から所定のデータを取り出すデータ取得手段と、データ取得手段により取得した暗号化されたデータを暗号鍵により復号する復号手段と、暗号鍵を保管する暗号鍵保管手段と、復号手段により復号されたデータを外部に出力する出力手段とを備える。

【００１１】このような構成を有するデータ受信装置は、受信手段により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル手段によりデスクランブル処理を施し、ディジタルデータにして取り出し、そして、当該ディジタルデータから、データ取得手段により、所定のデータを取り出す。

【００１２】そして、データ受信装置は、データ取得手段により取得した暗号化されているデータを、復号手段により暗号鍵を用いて復号する。さらに、データ受信装置は、このように復号した得たデータを出力手段により外部に出力する。

【００１３】これにより、データ受信装置は、スクランブル処理されて伝送されてくる信号から当該データ受信装置に宛てて送信された情報のみを意味のある情報として取り込むことができる。

【００１４】本発明に係るデータ受信方法は、上述の課題を解決するために、衛星通信路を介して配信される信号データを受信する受信工程と、信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出すデスクランブル工程と、ディジタル信号から所定のデータを取り出すデータ取得工程と、データ取得工程により取得した暗号化されたデータを、暗号鍵保管手段に保管されている暗号鍵により復号する復号工程と、復号工程により復号されたデータを外部に出力する出力工程とを有する。

【００１５】このデータ受信方法は、受信工程により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル工程によりデスクランブル処理を施し、ディジタルデータにして取り出し、そして、当該ディジタルデータから、データ取得工程により、所定のデータを取り出す。

【００１６】そして、データ受信方法は、データ取得工程により取得した暗号化されているデータを、復号工程により暗号鍵を用いて復号する。さらに、データ受信装置は、このように復号した得たデータを出力工程により外部に出力する。

【００１７】このデータ受信方法により、スクランブル処理されて伝送されてくる信号からデータ受信装置に宛てて送信された情報のみを意味のある情報として取り込むことができる。

【００１８】また、本発明に係るデータ送信方法は、上述の課題を解決するために、衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加するデータ暗号化工程と、暗号鍵を用いて暗号化されたデータ及び当該暗号化されたデータに付加されている配信先情報に対して、映像音声情報をスクランブル処理するのと同一のに処理によりスクランブル処理を行うスクランブル処理工程と、スクランブル処理された各種データを上記衛星通信路上に伝送するデータ伝送工程とを有する。

【００１９】このデータ送信方法は、データ暗号化工程により、衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加し、スクランブル処理工程により、当該データ及び情報に、映像音声情報のスクランブルに使用されるスクランブル処理を施し、データ伝送工程により、このスクランブル処理されたデータを上記衛星通信路上に伝送する。

【００２０】このデータ送信方法によりデータが配信されるデータ受信側では、スクランブル処理されて伝送されてくる信号から暗号化されている情報を上記宛先情報に基づいて取り出し、当該取り出した暗号化されているデータを暗号鍵により復号する。

【００２１】

【発明の実施の形態】以下、本発明に係るデータ受信装置について実施の形態について図面を用いて詳しく説明する。この実施の形態は、通信衛星を利用してテレビジョン放送等を行う、いわゆるブロードキャスト型のデータ伝送システムにおいて、当該テレビジョン放送とともに配信されるデータを受信することができるデータ受信装置に適用したものである。

【００２２】上記データ伝送システムは、図１に示すように、当該データ伝送システム１において契約者４に配信するデータを提供する情報提供者２と、情報提供者２から提供されたデータを所定の契約者４に送信する伝送路提供事業者であるサービス運用会社３と、上記サービス運用会社３のの契約により当該サービス運用会社３からデータが配信される各契約者４Ａ，４Ｂ，・・・，４Ｎが所有するデータ受信装置１０と、上記サービス運用会社３から契約者４へのデータの転送に用いられる通信衛星５並びに公衆電話回線及び専用線等の有線通信路１０と、各種情報を提供するとされるインターネット７とから構成される。このような形態とされるデータ伝送システム１は、例えば、現行のＣＳディジタル衛星放送と基本的には同様なシステム構成とされる。

【００２３】このように構成されているデータ伝送システム１において、契約者４Ａ，４Ｂ，・・・，４Ｎは、インターネット等において要求した情報の通信衛星５を介して配信するサービスが受けられる。

【００２４】上記情報提供者２は、契約を結んだ契約者４に対して各種データを提供するものあって、例えば、各種情報を保有している複数の情報提供者２ａ，２ｂ，・・・，２ｚから構成されている。この各情報提供者２ａ，２ｂ，・・・，２ｚは、契約者４Ａ，４Ｂ，・・・，４Ｎが要求した情報をサービス運用会社３により、当該情報要求した契約者４に配信する。

【００２５】上記インターネット７は、各種情報をいわゆる公衆電話回線等の通信回線を介して提供しているものでって、上記契約者４Ａ，４Ｂ，・・・，４Ｎが上記サービス運用会社３との契約によりアクセス可能とされる情報提供サービスである。例えば、インターネットにより、新聞情報、雑誌情報、音楽情報、ショッピング情報、インターネットWWW（World Wide Web）情報等が契約者４Ａ，４Ｂ，・・・，４Ｎに提供され、契約者４Ａ，４Ｂ，・・・，４Ｎは、コンピュータ等でインターネット上の各種情報を閲覧及び操作可能とされる。

【００２６】上記サービス運用会社３は、各情報提供者２ａ，２ｂ，・・・，２ｚが取り扱い及び発信する様々な情報を取りまとめ、通信衛星５又は有線通信路６を介して契約者７に情報を配信している。このサービス運用会社３は、送信アンテナ１２を備え、これにより、通信衛星５へのデータの伝送を行っている。上記通信衛星５を介することにより、サービス運用会社３は、一方向であるが大容量のデータの配信が可能になり、例えば３０Ｍｐｐｓの高速のデータ転送によるデータの転送が可能とされる。一方、サービス運用会社３は、有線通信路６を介することにより、契約者４Ａ，４Ｂ，・・・，４Ｎとの間で双方向でデータの送受信を行うことができるものの、上記通信衛星５を利用したものよりも小容量のデータ転送に留まる。

【００２７】ここで、上記サービス運用会社３は、上記通信衛星５を経由されて上記取りまとめた各種情報を契約者４Ａ，４Ｂ，・・・，４Ｎに配信する際には、衛星通信路５上におけるデータフォーマットを、サービス運用会社３の自由なフォーマットとしているのではなく、衛星テレビ放送に用いられているのと同様なフォーマットを採用している。例えば、サービス運用会社３は、欧州や日本等で運営されている衛星放送に採用されている現行のＤＶＢ（Digital Video Broadcasting）規格等の標準規格に準じたフォーマットに変換して、上記情報提供者２等から取りまとめた各種情報を上記通信衛星５に

伝送している。上記契約者４Ａ，４Ｂ，・・・，４Ｎは、コンピュータ１３に内蔵してデータ受信装置を有している。例えば、各契約者４Ａ，４Ｂ，・・・，４Ｎは、上記サービス運用会社３を契約した際に、上記データ受信装置の提供を受ける。

【００２８】本発明の実施の形態とれる上記データ受信装置は、図２に示すように、衛星通信上に伝送された信号を受信するための受信アンテナ８と、受信アンテナ８により受信された信号を処理する信号処理部９とから構成されている。このデータ受信装置１０は、例えば現行のＢＳテレビジョン放送やＣＳテレビジョン放送等において配信対象とされている映像や音声サービスのみならず、コンピュータ１３が扱うことができる情報を受信することが可能となるように構成されている。データ受信装置１０は、例えば現在一般的に普及されているコンピュータに内蔵するボードタイプとして構成され、受信アンテナ８からの同軸ケーブル３１がコンピュータ１３に内蔵された信号処理部９と接続されるような構造とされている。

【００２９】このような構成を有するデータ伝送システム１においては、上述したように、上記契約者４は、上記サービス運用会社３によりインターネット７のWWW情報が閲覧可能とされており、これにより、上記契約者４Ａ，４Ｂ，・・・，４Ｎは、当該インターネット７上に存在する各種情報の配信を要求する等のインタラクティブなサービスの提供を受けることができる。すなわち、データ伝送システム１は、通信衛星５の使用用途を現行のＢＳテレビジョン放送またはＣＳテレビジョン放送用以外にも上記インタラクティブなサービスを可能にするように構成されているシステムである。これにより、契約者４は、インターネット１０を閲覧して、欲しい情報があった場合、当該情報を通信衛星５を介して取得することが可能になる。

【００３０】例えば、このように通信衛星５を使用して個人が要求した情報を取得しようとする場合、有線通信路６におけるときと同様に秘密保持管理が当然要求される。すなわち、有線通信路６のように情報提供者と情報受信者（契約者）の双方向において、他の者にあっては、当該送受信の対象とされる情報が取得不可能又は意味がないような情報とされるような秘密保持管理が要求される。

【００３１】すなわち、上述したように、通信衛星５を利用してデータの配信を行おうとすれば、例えば、ある時刻において通信衛星路上には、現行のＢＳテレビジョン放送等のように契約者４Ａ，４Ｂ，・・・，４Ｎのみが見ることができる情報とともに、その中の一人の契約者、例えば契約者４Ａ、のためだけの情報が送信されることが起こる。このような場合でも、通信衛星５からの上記ＢＳテレビジョン放送を契約者４Ａ，４Ｂ，・・・，４Ｎの全員が受信可能とされる一方で、ある契約者（個人又は団体）のみが自分が契約した情報提供者から提供された情報を受信可能とされるような秘密保持管理が要求される。すなわち、上記ＢＳテレビジョン放送に関しては、契約者の全員４Ａ，４Ｂ，・・・，４Ｎが受信することを可能にしながら、契約者４Ａが配信要求した情報に関しては、契約者４Ａだけは当該配信された情報を意味のある情報として得ることができ、また、何ら当該情報を要求していない他の契約者である契約者４Ｂ，・・・，４Ｎは当該配信されてくる情報を意味のない信号として受信し、永久に意味のある情報として得ることができないような秘密保持管理が要求される。

【００３２】なお、契約者４からのリクエストにより行う情報の検索については、次にようになる。すなわち、契約者４Ａ，４Ｂ，・・・，４Ｎが、ある任意の時刻に、インターネット７上のWWW情報を閲覧して、その情報の内に欲しい情報があり、当該情報が欲しい場合に、データ受信装置１０を内蔵したコンピュータからモデムやイーサネット等により有線通信路６を経由して、情報のリクエスト命令をサービス運用会社３に発信する。特定の契約者４からの特定の情報のリクエストを受けたサービス運用会社３は、その情報の種別によりインターネット７にアクセス又は情報提供者２にアクセスして契約者４からの特定のリクエストの情報を得る。そして、サービス運用会社３は、得た特定の情報をその契約者しか受信できない形態に情報を変換して通信衛星５へのデータ伝送を行う。

【００３３】以上のように、従来のようにＢＳテレビジョン放送、及びリクエストにより、通信衛星５を介した契約者４への配信が行われる。次に、データ伝送システム１において衛星通信路上に打ち上げるための所定のデータフォーマットに基づいたデータ作成操作について、図３を用いて説明する。本例では、データ作成の操作を５段階にして説明する。なお、データフォーマットを、ＤＶＢ（Digital Video Broadcasting）規格として説明する。

【００３４】先ず、データ操作＜１＞として、情報提供者２からの情報21_1，・・・，21_n，・・・，21_{n+m}は、いわゆる素のデータの形でサービス運用会社３に配信される。ここで、情報提供者２からサービス運用会社３に配信される情報21_1，・・・，21_n，・・・，21_{n+m}は、上述したように、契約者４Ａ，４Ｂ，・・・，４Ｎのための情報、又はその内の一人の契約者がリクエストした情報である。すなわち、例えば、上述したように、契約者４Ａ，４Ｂ，・・・，４Ｎのための ＢＳテレビジョン放送の映像情報又はその一の契約者がインターネットにリクエストした情報である。そして、サービス運用会社３は、付加情報として各契約者へ配信すべき情報を、情報提供者２又はインターネット７から得ることにより、情報提供者２から受け取った情報21_1，・・・，21_n，・・・，21_{n+m}がどの契約者宛て

の情報であるかを知ることができる。例えば、サービス運用会社３には、ＩＰ（Internet Protocol）で規格化して上記各種情報を配信をする。すなわち、ＩＰパケットに上記情報21_1，・・・，21_n，・・・，21_{n+m}が格納され、そのＩＰパケットのヘッダ部（以下、ＩＰヘッダ部という。）に、当該各情報が配信されるべき各契約者にアドレス情報が格納される。例えば、ＩＰヘッダ部は、図４に示すように、ＩＰアドレス７４に配信先のアドレスを格納し、ＩＰアドレス７３に配信元のアドレスを格納している。

【００３５】次に、データ操作＜２＞として、上記データ操作＜１＞により得た情報21_1，・・・，21_n，・・・，21_{n+m}を、衛星通信路上でのデータフォーマットとして規定されているＭＡＣ（Media Access Control）フレームに変換する。ここで、ＭＡＣフレーム化することにより、通信衛星経路上でのデータの伝送制御が可能となる。このＭＡＣフレーム化により、伝送対象となる各情報21_1，・・・，21_n，・・・，21_{n+m}がデータパケットP_Dに格納され、このデータパケットP_Dに伝送制御情報が格納されるＭＡＣヘッダH_{MAC}が付加される。

【００３６】ここで、上記各情報は、上述したように、宛先が予め決定されており、例えば、上記情報21_1は、契約者４Ａが要求した情報であり、上記情報21_nは、全契約者４Ａ，４Ｂ，・・・，４Ｎが要求した情報であり、そして上記情報21_{n+m}は、契約者４Ｂのための情報である。そして、上記データパケットP_Dは、ここで、暗号鍵による暗号化処理が施されている。すなわち、上記各情報21_1，・・・，21_n，・・・，21_{n+m}が暗号化処理される。暗号鍵による暗号化処理とは、所定の情報に対して暗号鍵を用いて暗号化することをいう。そして、この暗号鍵により暗号化処理された情報は、当該暗号鍵に対応した復号鍵により解除され、読み取ることが可能となる。ここで、上記復号鍵は、データ受信装置１０により各契約者が保持しているものである。

【００３７】すなわち、サービス運用会社３は、各契約者のみが持つ暗号鍵を保持し、情報提供者２から配信された所定の契約者のみに配信したい情報を、当該配信を要求している契約者が保持している復号鍵に対応される暗号鍵により暗号化している。契約者４Ａのための上記情報21_1は、契約者４Ａが保持している復号鍵に対応した暗号鍵を用いて暗号化処理を行い、また、全契約者４Ａ，４Ｂ，・・・，４Ｎのための上記情報21_nは、契約者４Ａ，４Ｂ，・・・，４Ｎの全員が有している復号鍵に対応された暗号鍵を用いて暗号処理を行い、そして、契約者４Ｂのための上記情報21_{n+m}は、契約者４Ｂが有する復号鍵に対応された暗号鍵を用いて暗号化処理を行っている。

【００３８】このように、情報を要求した契約者に応じて暗号鍵を使いわけることにより、各契約者が保持している上記復号鍵は互いに異なっていることから、一の契約者のための暗号鍵により暗号化され、配信される情報が他の契約者が保持している上記復号鍵では復号することができなくなる。なお、各契約者の復号鍵は、サービス運用会社３から伝送されるものであり、例えば、当該伝送を定期的に行うことにより、安全が図られている。

【００３９】なお、上記ＭＡＣヘッダH_{MAC}には、当該情報を伝送すべき契約者の宛先を示すアドレスや、暗号化がされているかどうかを示す制御コードが格納されている。このＭＡＣヘッダH_{MAC}は、暗号鍵による暗号化処理が施されない部分であって、受信側である各データ受信装置１０では、復号鍵により復号化を要することなく、このＭＡＣヘッダH_{MAC}を参照して、自分宛てのデータかどうかを識別することになる。例えば、図５に示すように、ＭＡＣヘッダ７０は、８ビットのＳＳＩＤ（Server System ID）と、２４ビットのＵＤＢ（User Depend Block）１と、３２ビットのＵＤＢ２の計６４ビットで構成されている。特に、ＭＡＣヘッダ７０のＵＤＢ２には、上記ＩＰヘッダ内に書かれた送信先ＩＰアドレスと同様の配信先のＩＰアドレスが書き込まれる。このＭＡＣヘッダ７０に格納されている配信先のＩＰアドレスにより、受信側では単にハードウェア的にそれを読み出すことで、自分宛のデータパケットであるか否かを知ることができる。

【００４０】そして、データ操作＜３＞として、上記データ操作＜２＞によって生成されたＭＡＣフレームは、衛星通信路上に配信するためのＭＰＥＧ２（Moving PictureExperts Group Phase 2）規格によるデータストリーム化がなされる。このＭＰＥＧ２規格によるストリーム化により、ＭＡＣフレーム23_1，・・・，23_n，・・・，23_{n+m}には、ＭＰＥＧ２ヘッダH_{MPEG}及びフッタＦが付加される。

【００４１】ここでのＭＰＥＧ２ストリーム23_1，・・・，23_n，・・・，23_{n+m}は、例えばプライベートセレクション（Private Section）と呼ばれるデータフォーマットによって規定されるデータストリームであって、ＭＰＥＧ２により標準フォーマットが規定されるものである。そして、上記ＭＰＥＧ２ヘッダH_{MPEG}は、サービス運用会社３のベンダーＩＤや一つのＭＰＥＧ２ストリームの長さ等の制御情報を格納している。また、上記フッタＦは受信側で衛星通信路上で一部ビットの損失もなく正常に情報が配信されたかどうを知るための制御コードであって、例えばＣＲＣ（Cyclic Redundancy Check）によって付加されるコードである。このＣＲＣによるコードを付加することにより、受信側では、受信したＭＰＥＧ２ストリームを先頭からＣＲＣ計算を行い、当該ストリームの最後までの計算結果が付加されているフッタＦの値と一致したときにのみ、受信したＭＰＥＧ２ストリームが正常に受信できたと認識することができ

るようになる。

【００４２】そして、データ操作＜４＞として、上記データ操作＜３＞により生成された各ＭＰＥＧ２ストリーム23_1，・・・，23_n，・・・，23_{n+m}を、衛星通信路上に配信するために、上記ＤＶＢの規定に従って、ＭＰＥＧ２によるＴＳパケット（トランスポートストリームパケット）化を行う。

【００４３】上記ＴＳパケット化により、各ＭＰＥＧ２ストリーム23_1，・・・，23_n，・・・，23_{n+m}は、複数のペイロードデータ部とされてＴＳパケットP_{TS}に分割されて格納され、各ＴＳパケットP_{TS}には、４バイトのＴＳヘッダH_{TS}が付加される。

【００４４】ここで、上記ＴＳパケットP_{TS}及びＴＳヘッダH_{TS}により構成されるパケット24_1，24_2，24_3，・・・，24_{K-2}，24_{K-1}，24_Kは、８８バイトの固定長として構成され、ここでは、格納されるＭＰＥＧ２ストリームが大きいため、複数のＴＳパケットとされている。

【００４５】上記ＴＳヘッダH_{TS}には、当該ヘッダ以降続くデータのための制御データが格納されており、具体的には、当該ヘッダ以降続くデータがサービス運用会社３から配信された制御データ又は契約者４が要求した情報かの識別を示すコード、若しくはそのＴＳパケットP_{TS}が分割されたＭＰＥＧ２ストリームの先頭か途中かを示す制御コードが格納されている。なお、上述したように、ＴＳヘッダH_{TS}により行うサービス運用会社３から配信された制御データか否かの識別は、サービス運用会社３が当該データを受信するデータ受信装置１０に対して制御データを送ることがあるためである。

【００４６】そして、データ操作５において、上記データ操作４で生成されたパケット24_1，24_2，24_3，・・・，24_{K-2}，24_{K-1}，24_Kは、衛星通信路上に配信するために必要な変調、例えばＱＰＳＫ（Quadrature PSK）変調、スクランブル処理等されたパケット25_1，25_2，25_3，・・・，25_{K-2}，25_{K-1}，25_Kとして通信衛星５に伝送される。

【００４７】以上のように、データ伝送システム１において所定のデータフォーマットに基づいたデータ作成操作が行われて、通信衛星５へのデータの伝送が行われる。

【００４８】次に、上述のように生成されて、通信衛星５による衛星通信路上に伝送されたデータのデータ受信装置１０側における処理について説明する。

【００４９】上記データ受信装置１０は、図２に示すように、上記通信衛星５を介して配信される信号データを受信する受信手段を構成する受信アンテナ８及び同軸ケーブル３１と、前記受信手段を構成し、上記信号データに施されたスクランブル処理に応じてデスクランブルしてディジタル信号を取り出すデスクランブル機能を有する衛星データ取り込み装置３２と、上記ディジタル信号から所定のデータを取り出すデータ取得機能、当該データ取得機能により取得したディジタルデータを暗号鍵により復号する復号機能及び上記復号鍵を管理する復号鍵管理機能を有するデータ復号装置３３と、データ復号装置により復号されたデータを外部に出力する出力手段を構成する受信データ出力Ｉ／Ｆ装置３５とを備えている。なお、ここで、衛星データ取り込み装置３２、データ復号処理装置３３、データ入力装置３８、受信データ出力Ｉ／Ｆ装置３５及び全体制御装置３４により上記信号処理部９を構成している。

【００５０】また、データ受信装置１０は、汎用衛星放送受信端末３９から出力される当該データ受信装置１０とのインターフェースとされるデータ入力装置３８と、当該データ受信装置１０全体を制御する全体制御装置３４とを備えている。

【００５１】そして、データ受信装置１０は、コンピュータ内部バス３６に接続され、このコンピュータ内部バス３６を介してコンピュータ内部ＣＰＵ３７との間で各種データの送受信を行っている。

【００５２】ここで、データ受信装置１０に接続されている上記汎用衛星放送受信端末３９は、例えば上述したようにＢＳテレビジョン放送用の受信端末である。

【００５３】以下、上記データ受信装置１０を構成する各部について説明する。

【００５４】上記受信アンテナ３０は、衛星通信路上のデータを当該データ受信装置１０に取り込むための受信手段を構成している。この受信アンテナ３０により受信したデータは、上記同軸ケーブル３１を介して当該データ受信装置１０の本体に入力される。ここで、入力されたデータは、ＩＦ信号データであって、ＩＦ信号データには、各契約者に配信されるデータと同じ、すなわち、当該ＩＦ信号データを受信した契約者が要求した情報以外の情報も全て含まれている。例えば、ＩＦ信号データは、データ受信端末用の制御情報や、他契約者宛ての情報である。

【００５５】上記衛星データ取り込み装置３２は、入力されたＩＦ信号データについて、ＴＴＬ（Time to Live）レベルにディジタルデータ化する装置であって、ＡＤ変換や信号の同期取りなどのディジタル衛星放送受信のために必要不可欠な最低限の処理を行うように構成されている。この衛星データ取り込装置３２は、入力されてデータに対してデスクランブル処理を施し、上記ＴＳパケットP_{TS}からＭＰＥＧ２ストリームを再構築し、ＭＰＥＧ２ストリームとされたディジタルデータとして出力する。このデータ取り込み装置３２から出力された上記ＭＰＥＧ２ストリームは、上記データ復号装置３３に入力される。

【００５６】データ復号装置３３は、入力されたＭＰＥＧ２ストリームについて復号処理を行うように構成されている。このデータ復号装置３３は、ＭＰＥＧ２ストリ

ームの中のＭＡＣアドレス（宛先アドレス）と、全体制御装置３４によって指定されたＭＡＣアドレスとを比較し、その比較結果が一致し、かつそのストリームが暗号されている場合に、当該ＭＰＥＧ２ストリームについて復号処理を行う。これに対し、データ復号装置３３は、受信したばかりのＭＰＥＧ２ストリーム内のＭＡＣアドレスと一致したものがなければその場で当該受信したＭＰＥＧ２ストリームを破棄する。このデータ復号装置３３は、実時間で暗号化されたデータの復号処理を行っており、これにより、大容量のデータを高速で復号することを実現している。

【００５７】上記データ復号装置３３により復号されたＭＰＥＧ２ストリームは、そのヘッダとされるＭＰＥＧ２ヘッダH_{MPEG}とＭＡＣヘッダH_{MAC}が取り除かれた段階で受信データ出力Ｉ／Ｆ装置３５に出力される。

【００５８】上記受信データ出力Ｉ／Ｆ装置３５は、当該データ受信装置１０とコンピュータ１３とのインターフェースとして構成されている。この受信データ出力Ｉ／Ｆ装置３５は、正常に復号できたデータパケットをコンピュータ内部バス３６に出力する。なお、受信データ出力Ｉ／Ｆ装置３５は、そのデータ受信装置１０を内蔵しているコンピュータ内部バス３６のプロトコルを守るロジックを持っている。

【００５９】上記全体制御装置３４は、データ受信装置１０の全体を監視及び管理するように構成されている。例えば、具体的には、データ受信装置１０が接続されるコンピュータ１３のアプリケーションからの制御命令や受信したデータの中に入っているデータ受信装置１０の制御用のデータを解釈して、データ受信装置１０全体の監視及び管理を行う。

【００６０】上記汎用衛星放送受信端末３９は、例えば衛星テレビジョン放送用の受信端末であって、例えば、現存するＢＳテレビジョン放送やＣＳテレビジョン放送等に用いられるものである。上述したように、サービス運用会社３は、上記ＢＳテレビジョン放送等とともに情報提供者２から配信された各種情報を加工したデータとして衛星通信路上に伝送しており、汎用衛星放送用受信端末３９は、上記ＢＳテレビジョン放送と、当該ＢＳテレビジョン放送とともに伝送されるデータをも入力されるように構成されている。

【００６１】そして、データ受信装置１０は、上記汎用衛星放送受信端末３９とのインターフェースとして図示しない接続Ｉ／Ｆを持っており、これにより、接続される上記汎用衛星放送受信端末３９からデータの入力が可能とされている。

【００６２】このように、上記汎用衛星放送受信端末３９とのインターフェースとして上記接続Ｉ／Ｆを持つことにより、データ受信装置１０は、上記受信アンテナ８等を有していない場合であっても、上記汎用衛星放送受信端末３９からデータの入力を可能とし、将来的な汎用

性を持つことができる。なお、この場合、上述したように上記衛星データ取り込み装置３２からデータ復号装置３３へのデータの出力がなくなり、データ入力装置３８からデータがデータ復号装置３３に入力されることになる。

【００６３】上記データ受信装置１０については、詳しくは、図６に示すように構成されている。この図６に示すデータ受信装置１０を用いて受信されてデータの処理について詳しく説明する。なお、ここでは、契約者４Ａにおけるデータの受信について説明する。

【００６４】上記受信アンテナ８により受信された受信ＩＦ信号データ１０１は、契約者４が要求した情報21_1，・・・，21_n，・・・，21_{n+m}と、それ以外のデータ、例えば上記ＢＳテレビジョン放送とを構成するデータとからなり、例えば、データ受信装置１０の制御用情報や、他契約者宛ての情報も含まれているデータである。ここで、ＩＦ信号データは、上記図７に示すデータ操作＜６＞に示すように、スクランブル処理されたパケット25_1，25_2，25_3，・・・，25_{K-2}，25_{K-1}，25_Kとされる。

【００６５】このＩＦ信号データ１０１は、上記衛星データ取り込み装置３４によって、ＡＤ変換、信号の同期取りデスクランブル処理等の、ディジタル衛星放送受信のために必要不可欠な最低限の処理が施され、最終的にＴＳパケット１０２として出力され、ＭＰＥＧ２ストリーム回復装置５１に入力される。すなわち、ここでは、上記図７に示すように、データ操作＜７＞として、パケット24_1，24_2，24_3，・・・，24_{K-2}，24_{K-1}，24_Kのスクランブル処理を行う。

【００６６】上記ＭＰＥＧ２ストリーム回復装置５１は、送信側においてＴＳパケット１０２として分割されたＭＰＥＧ２ストリームの回復作業を行うように構成されている。このＭＰＥＧ２ストリーム回復装置５１が行うＭＰＥＧ２ストリームの回復作業は、ＴＳパケット１０２の先頭のＴＳヘッダH_{TS}内の制御コードを参照することにより、分割されているＭＰＥＧ２ストリームの先頭を検出して、一つのＭＰＥＧ２ストリーム１０３を生成している。すなわち、上記図７に示すように、データ操作＜８＞として、ＭＰＥＧ２ストリーム23_1，・・・，23_n，・・・，23_{n+m}を生成する。このＭＰＥＧ２ストリーム回復装置５１により回復されたＭＰＥＧ２ストリーム１０３は、ＭＰＥＧ２ストリーム検査装置５２に入力される。

【００６７】ＭＰＥＧ２ストリーム検査装置５２は、ＭＰＥＧ２ストリーム１０２に衛星通信路上でのノイズが発生しているか否かを検査する作業と、ＭＰＥＧ２ストリーム１０２のフィルタリング（振り分け）作業と、大きく分けて２つの作業を行うように構成されている。

【００６８】ＭＰＥＧ２ストリーム検査装置５２において行う衛星通信路上でのノイズの発生の検査は、ＭＰＥ

Ｇ２ストリーム１０３のフッタＦに付随されたＣＲＣの値を用いて行っている。すなわち、ＭＰＥＧ２ストリーム検査装置５２は、入力されたＭＰＥＧ２ストリーム１０３の先頭から最後までＭＰＥＧ２により規定されているＣＲＣの計算を施し、最後まで計算したＣＲＣの値と、送信側においてＭＰＥＧ２ストリーム１０３のフッタＦに付随されたＣＲＣの値を比較して、同等であった場合のみ、「エラーなく通信できたパケット」として判断する。ここで、判断処理がなされたＭＰＥＧ２ストリーム１０４は、ＭＰＥＧ２ストリーム破棄装置５３へ送られる。なお、ここで、ＣＲＣの計算は入力されたＭＰＥＧ２ストリーム１０３の最後まで行われるので、判定が決まるまではデータ一時蓄積装置５４に保管される。

【００６９】ＭＰＥＧ２ストリーム破棄装置５３は、ＣＲＣにより計算エラーが発生したＭＰＥＧ２ストリームについて破棄処理を行うように構成されている。具体的には、ＭＰＥＧ２ストリーム検査装置５２から送られてくるストリーム破棄命令１０６により、当該ストリーム破棄命令１０６に対応されるＭＰＥＧ２ストリームの破棄を行う。そして、ＣＲＣの計算エラーにより破棄したＭＰＥＧ２ストリームがあった事実は、破棄した旨として全体制御装置３４に報告される。

【００７０】また、ＭＰＥＧ２ストリーム検査装置５２において行うＭＰＥＧ２ストリームのフィルタリングは、ＭＰＥＧ２ストリーム回復装置５１から送られたＭＰＥＧ２ストリーム１０３が、データ受信装置１０の所有者である契約者４Ａが要求した情報か否かを審査して、必要ならば後段のＭＰＥＧ２ストリーム破棄装置５３に送り、不要であればその場でＭＰＥＧ２ストリーム１０３の破棄の処理を行うように構成されている。

【００７１】具体的には、ＭＰＥＧ２ストリーム検査装置５２は、ＭＰＥＧ２ストリーム内のＭＡＣフレーム内のＭＡＣヘッダH_{MAC}に格納されている宛先アドレスと、全体制御装置３４からセットされる当該データ受信装置１０自身がその時刻で保有しているアドレスとを比較して、受信すべきＭＰＥＧ２ストリームと判断された時のみ、そのＭＰＥＧ２ストリームをＭＰＥＧ２ストリーム破棄装置５３に出力する。通常、自分が持つアドレスは同時に数種類であり、それ以外のアドレスを宛先とするＭＰＥＧ２ストリームはＭＰＥＧ２ストリーム検査装置５２において破棄されることになる。

【００７２】よって、上記ＭＰＥＧ２ストリーム検査装置５２により行った上記２つの作業により破棄されなかったＭＰＥＧ２ストリームは、エラーなく正常に自分宛てに伝送されてきたデータであり、すなわち、自分自身が受け取るべきストリームである。なお、全体制御装置３４によってセットされる自分のアドレスは、時刻と共に変化する可能性がある。

【００７３】上述のように、暗号化されていないＭＡＣヘッダH_{MAC}に格納されている宛先アドレスを確認することにより、復号化するなどの無駄な処理を要しなくても当該ＭＡＣヘッダH_{MAC}が付加されている情報が自己宛に送られてきた情報か否かを瞬時に判断することができるようになる。これは、以降に続いて入力されてくるＭＰＥＧ２ストリームは遅滞なく処理するを可能にする。

【００７４】なお、ＭＰＥＧ２ストリーム検査装置５２は、入力されたＭＰＥＧ２ストリーム１０３からヘッダH_{MPEG}及びフッタＦを取り除いた形のＭＰＥＧ２ストリーム１０４のデータとしてデータ一時蓄積装置５４に出力している。すなわち、上記図２に示すように、データ操作９として、ＭＰＥＧ２ストリーム22_1，・・・22_n，・・・，22_{n+m}としてデータ一時蓄積装置５に出力している。

【００７５】そして、データ一時蓄積装置５４から出力されて、ＭＰＥＧ２ストリーム破棄装置５３において破棄されずに通過したフッタＦなしのＭＰＥＧ２ストリーム１０７は、復号鍵検索装置５５に入力される。

【００７６】復号鍵検索装置５５は、入力されてきたＭＰＥＧ２ストリーム１０７に対する暗号鍵を検索するように構成されている。具体的には、復号鍵検索装置５５は、暗号化されたユーザのためのデータの先頭のヘッダ情報を見て復号に必要な復号鍵を、データパケット（かたまり）毎に実時間で検索及び設定する。すなわち、復号鍵検索装置５５は、ＭＰＥＧ２ストリーム１０７内のＭＡＣヘッダH_{MAC}内の、暗号がかけられているかどうかを示す制御ビットを見て、入力されたばかりのＭＰＥＧ２ストリーム１０７内の情報21_1，・・・，21_n，・・・，21_{n+m}に暗号処理が施されているか否かを判別し、これに基づいて、復号鍵保管部５６における復号鍵の検索等を行う。

【００７７】ここで、暗号処理が施されていないことを確認した場合には、後段の復号装置５８に対して復号しない命令とともに当該暗号処理が施されていないＭＰＥＧ２ストリームが復号鍵検索装置５５から出力される。なお、復号装置５８に出力されるＭＰＥＧ２ストリームは、これまで付加されていたＭＰＥＧ２ヘッダH_{MPEG}及びＭＡＣヘッダH_{MAC}が取り除かれ、素の状態とされた情報21_1，・・・，21_n，・・・，21_{n+m}のデータパケットP_Dとして出力される。すなわち、上記図２に示のデータ操作１０に示すように、情報21_1，・・・，21_n，・・・，21_{n+m}によって構成されるデータパケットして出力される。

【００７８】また、暗号処理が施されていることを確認した場合には、復号鍵検索装置５５は、ＭＰＥＧ２ストリーム１０７内のＭＡＣヘッダH_{MAC}内の宛先アドレスに基づいて、復号鍵保管部５６に復号鍵の要求命令１０９を出す。

【００７９】復号鍵保管部５６は、ある時刻においてデータ受信装置１０を保有する契約者が受信することが許

可されているデータを復号するための復号鍵を保管している。この復号鍵保管部５６は、例えばメモリにより構成されている。

【００８０】また、復号鍵保管部５６は、複数の復号鍵を保管することも可能とされており、それらの復号鍵は、全体制御装置５６により管理されている。この復号鍵保管部５６は、上記復号鍵の要求命令１０９により、対応した復号鍵を復号鍵検索装置５５に出力する。例えば、復号鍵保管部５６には、随時変更される可能性があるセッション鍵及び恒久的に保管されるマスター鍵が少なくとも含まれている。

【００８１】ここで、セッション鍵とは、特定のサービス運用会社から送信されて情報を復号するための復号鍵であり、さらに、通常は、日毎、時間毎、ファイル毎、サービス毎等に逐次変化するものとされている。また、上記マスター鍵は、例えば、データ受信装置固有の復号鍵であって、例えば、上記セッション鍵を復号するために使用される。よって、このような場合には、マスター鍵により先ずセッション鍵を復号してから、当該セッション鍵により上記暗号化された情報の復号を行う。このように行うことに、情報の秘密保持を向上させることができるようになる。

【００８２】そして、復号鍵保管部５６に保管される復号鍵は、鍵設定部５７により設定される。例えば、鍵設定部５７は、配信されてくる復号鍵を復号鍵保管部５６にセットすることや、上記復号鍵保管部５６に復号鍵を設定することができる。例えば、鍵設定部５７は、配信されてくる復号鍵を、コンピュータ内部バス３６から、受信データ出力Ｉ／Ｆ装置３５を介して得ることができ、全体制御装置３４の制御により、復号鍵保管部５６にセットする。例えば、このようにして復号鍵保管部５６にセットされる復号鍵は、上記セッション鍵である。また、鍵設定部５７は、工場出荷時に入力されるＩＤ等に基づいて、復号鍵保管部５６に鍵を設置することができる。例えば、このように工場出荷に設定される復号鍵は、上記マスター鍵の少なくとも一部として用いられる。

【００８３】上記復号鍵検索装置５５は、復号鍵保管部５４かれ送られてきた復号鍵及び当該復号鍵により暗号処理が解除されるＭＰＥＧ２ストリーム１０８を復号装置５８に出力する。なお、復号鍵検索装置５５から出力されるＭＰＥＧ２ストリームは、これまで付加されていたＭＰＥＧ２ヘッダH_{MPEG}及びＭＡＣヘッダH_{MAC}が取り除かれ、素の状態とされた情報21_1，・・・，21_n，・・・，21_{n+m}、すなわち、データパケットP_Dの状態とされて、復号装置５８に入力される。

【００８４】なお、上記復号鍵検索装置５５が受け取ったＭＰＥＧ２ストリームとされたデータパケットP_Dを復号するための復号鍵が上記復号鍵保管部５６に存在しない場合には、復号鍵検索装置５５は、そのＭＰＥＧ２

ストリームについての復号は不可能であることから、そのＭＰＥＧ２ストリームを破棄する。そして、このように復号鍵が保持していないことによりＭＰＥＧ２ストリームの破棄を行って場合には、その旨を全体制御装置３４に報告する。

【００８５】復号装置５８は、復号鍵検索装置５５からの受け取った復号鍵により、当該復号鍵とともに入力されたデータパケットP_Dの復号、すなわち暗号処理の解除を行うように構成されている。すなわち、復号装置５８は、復号鍵により暗号化されているデータパケットP_Dについて復号を行い、これにより、上記図７のデータ操作＜１０＞に示すように、契約者４Ａ及び全契約者のために転送されてきた情報21_1及び情報21_nのみを得ることができる。

【００８６】なお、上述したように、復号鍵検索装置５５は、暗号化されていないデータパケットについても復号装置５８に出力しており、よって、復号装置５８は、そのようなデータパケットが入力された場合については、復号鍵による復号をする必要がないので、何ら復号処理を施さずにその当該入力されたデータパケットを後段の復号後処理部兼パケット破棄装置５８に出力する。

【００８７】また、復号装置５８では、入力されるデータパケット毎に、逐一復号鍵の更新入力を受け取り処理することが可能な能力を持つ。これにより、ある契約者４が複数の復号鍵を同時刻に保有していたとしても、対応可能である。また、復号鍵検索装置５５からの命令によって、復号装置５８は、様々な初期値や複数の暗号モードをデータパケット毎に切り替えることが可能となる。

【００８８】復号装置５８は、復号が終了したデータパケット１１１又は復号をする必要がなかったデータパケット１１１を、後段の復号後処理部兼パケット破棄装置５９に出力する。

【００８９】なお、上述したように、暗号処理された情報を復号するための部分として復号鍵保管部５６、復号鍵検索装置５５及び復号装置５８をハードウェアとして構成することにより、実時間で暗号された情報の復号処理を実現することができる。

【００９０】復号後処理部兼パケット破棄装置５９は、データパケット１１１が復号装置５８において正しく復号できた否かを検査する。なお、データパケット１１１は、汎用のインターネット用のパケットとされるＩＰパケットであるが、復号後処理部兼パケット破棄装置５９は、正しく復号できたか否かを検査を、ＩＰパケットのヘッダにあるヘッダチェックサム等の計算をする等、ＩＰパケット内部のコードを主に用いて行っている。

【００９１】ここで、復号が正常に行われたことを確認した場合には、復号後処理部兼パケット破棄装置５９は、当該データパケット１１２のみを後段のデータ一時蓄積装置６０に出力する。また、復号が正常に行われた

なかったことを確認した場合には、復号後処理部兼パケット破棄装置５９は、当該データパケットを破棄し、その旨を全体制御装置３４に報告する。

【００９２】データ一時蓄積装置６０内に貯えられたデータパケット１１２は、上記受信データ出力Ｉ／Ｆ装置３５を介して、コンピュータのコンピュータ内部バス３６に入力される。

【００９３】また、上記図２に示すデータ受信装置１０のデータ入力装置３８は、図６に示す汎用衛星放送受信端末接続Ｉ／Ｆ６１と汎用衛星放送受信端末接続Ｉ／Ｆ６２とから構成されている。ここで、汎用衛星放送受信端末接続Ｉ／Ｆ６１は、いわゆるＴＴＬによるディジタルデータのインターフェースであり、また、汎用衛星放送受信端末接続Ｉ／Ｆ６２は、いわゆるＩＥＥＥ１３９４によって規格されたインターフェースである。

【００９４】そして、汎用衛星放送受信端末接続Ｉ／Ｆ６１及び汎用衛星放送受信端末接続Ｉ／Ｆ６２は、衛星データ取り込み装置３２と同時に作動することがないように構成されている。これにより、データの受信は、受信アンテナ３０を介した衛星データ取り込み装置３２か、汎用衛星放送受信端末接続Ｉ／Ｆ６１又は汎用衛星放送受信端末接続Ｉ／Ｆ６２かのいずれか一方の装置により当該データ受信装置１０に取り込まれることになる。すなわち、衛星データ取り込み装置３２によりデータが取り込まれている最中にあっては、汎用衛星放送受信端末接続Ｉ／Ｆ６１，６１の作動はなく、そして、逆も同じとされている。例えば、図８で示すように、受信アンテナ７０により受信されて衛星テレビジョン放送が同軸ケーブル７１を介して汎用衛星放送受信端末３９に入力された場合には、衛星データ取り込み装置３２は作動しないことになる。

【００９５】上記汎用衛星放送受信端末３９は、多チャンネルのＢＳテレビジョン放送等のデジタル衛星放送を受信することができる受信端末であって、例えばＩＲＤである。そして、上述したように、サービス運営会社３から伝送される情報を受信可能に構成されている。

【００９６】ところで、上述したように通信衛星５を利用して各種データの配信を行うサービス運営会社３については、他に存在するような場合であっても、サービス運営会社間に関してまったく異質なものではなく、統一化が図られるのが現状である。このことは、ユーザが、上記ＩＲＤといった一つの汎用衛星放送受信端末３９により複数のサービス運用会社３からの情報配信を受けることができる可能性を示唆している。よって、汎用衛星放送受信端末３９により、データ受信装置１０は、複数の送信先の異なるデータを受信することができるような構成が可能になる。このような場合に対応して、例えば、汎用衛星放送受信端末３９に入力されたデータが当該汎用衛星放送受信端末３９において何らかのデータの細工、例えばＩＣカードによる１次課金を処理する等がなされた後に、データ受信装置１０に入力したいといったデータの配信形態が今後出てくる可能性も考えられる。

【００９７】上記汎用衛星放送受信端末接続Ｉ／Ｆ６１，６２はこのような事態を解決するものであって、すなわち、データ受信装置１０は、汎用衛星放送受信端末接続Ｉ／Ｆ６１，６２が汎用性を持つインターフェースとして構成されることにより、あらゆる形態で配信されてくるデータを受信することができるようになる。これにより、異なったサービス運営会社による一般の衛星放送と衛星データ放送/通信サービスの共存が可能になる。なお、データ受信装置１０は、上述したように２種類の汎用衛星放送受信端末接続Ｉ／Ｆ６１，６２に限定されることはなく、数、インタフェースのプロトコルも適宜決定される。

【００９８】なお、上記全体制御装置３４は、上述したような制御を行う他に主に次のような機能を有している。

【００９９】全体制御装置３４は、データ受信装置１０全体のリセット及びイニシャライズを行う機能を有している。

【０１００】また、全体制御装置３４は、データ受信装置１０全体の状態監視と、その情報をコンピュータ内アプリケーションに報告する機能を有している。

【０１０１】さらに、全体制御装置３４は、ＭＰＥＧ２ストリーム検査装置５２へのＭＡＣアドレスの制御命令を行う。

【０１０２】そして、全体制御装置３４は、復号鍵保管部５６への復号鍵のセットをセット命令によって行う機能を有している。

【０１０３】また、全体制御装置３４は、各部からのパケット破棄報告の受信と、コンピュータ内アプリケーションへのその破棄の報告を行う機能を有してる。

【０１０４】さらに、全体制御装置３４は、その他、データ受信装置１０内のすべての作業を統括して管理するするように構成されている。

【０１０５】以上のように、データ受信装置１０は構成されている。このデータ受信装置１０は、信号処理装置９を構成する各部を一つの基板上に形成している。これにより、データ受信装置１０は、実時間でスイッチングする機能等により同一のハードウェアで効率よく各機能を実行させることが可能になる。

【０１０６】なお、上述したように、通信衛星５により配信されたデータを受信したデータ受信装置１０が、当該受信したデータから所定の情報のみを取り出す処理については、図７を用いると、次のように説明することができる。

【０１０７】なお、基本的には、ここで説明するデータ処理の流れは、上記図３を用いてデータ操作＜１＞～データ操作＜５＞として上記説明した処理手順と逆にな

る。しかし、受信側でのデータ操作において注意すべき点は、データ操作＜６＞からデータ操作＜１０＞に進むに従い、データ受信装置１０を構成する各ブロックにおいてデータが欠落していく可能性があることである。すなわち、所定の契約者、ここでは例えば契約者４Ａとは何ら関係のないデータが破棄されるということである。

【０１０８】すなわち、例えば、契約者４Ａにとっては、自分が持つデータ受信装置１０によって、受信した全ての衛星通信路上のデータの信号から次々と様々な要因でデータが破棄されていき、最終的に「正常に受信できた信号の中で、しかも契約者Ａのみが本来受け取れるべき情報」のみが、契約者４Ａにとって意味ある形となって受信される。具体的に、契約者４Ａが受信した衛星通信路上の全ての情報の中で、破棄される可能性のあるデータとして以下の複数ケースが考えられる。

【０１０９】データ操作＜６＞においては、衛星通信路上においてノイズが乗り、受信したデータが正常に復調できない場合、ストリームは破棄される。

【０１１０】そして、データ操作＜７＞においては、ＴＳヘッダHTS内の、制御データか情報かを示す識別ビットによって、ある契約者が要求する情報のみが取り込まれ制御データの方は破棄される。なお、ここでは、制御データが破棄されるというよりもデータ受信装置１０がある機能への命令として取り込まれた後に破棄されることが多いといえる。

【０１１１】さらに、データ操作＜８＞としては、ＭＰＥＧ２ストリームのＭＰＥＧ２フッタＦにある各ストリームのＣＲＣの計算結果が異なった場合、ＭＰＥＧ２ストリームがそのまま破棄される。例えば、ここでの破棄の原因は、衛星通信路上でノイズが乗ったためであると考えられる。

【０１１２】そして、データ操作＜９＞においては、他の契約者宛ての情報であるために、ＭＡＣフレーム内のＭＡＣヘッダHMAC内に、自分宛ての宛先のものが存在しないためにパケット又はストリームが破棄される。または、自分宛てのＭＡＣフレームであるが、システムが正常に動作していないなどの理由により、復号時に必要な復号鍵を保有していないため、又は、復号すべき鍵もあるが、データ受信装置内の復号装置もしくはその周辺装置の不具合により生じる可能性があるので、復号に失敗したなどの理由によりパケット又はストリームが破棄される。このようにデータ操作９において破棄される可能性があるパケットが一番多い。

【０１１３】上記データ受信装置１０は、通信衛星５からのデータを受信し、復号鍵保管検索装置５５が保管されている受信データ用の刻々変化しうる復号鍵を瞬時に検索し、復号装置５８が実時間かつ高速に受信データを復号し、受信データ出力Ｉ／Ｆ装置３５が高速にデータを外部に出力する等の、複数のブロックを同時に備え持つことにより、一人のユーザが本人のみ受信したい、又は送り手側がある特定のユーザにのみ配信したい機密性が高く大容量で多種類の衛星受信データをあるユーザが実時間で同時に受信することが可能になる。さらに、データ受信装置１０により、上記特徴と同時に、汎用データ入力用インタフェース部とされる汎用衛星放送受信端末接続Ｉ／Ｆ６１，６２を備えることにより、現行及び将来の多様な衛星放送サービスへの柔軟な対応が可能になる。

【０１１４】

【発明の効果】本発明に係るデータ受信装置は、受信手段により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル手段によりデスクランブル処理を施し、ディジタルデータにして取り出し、そして、当該ディジタルデータから、データ取得手段により、所定のデータを取り出すことができる。そして、データ受信装置は、データ取得手段により取得した暗号化されているデータを、復号手段により暗号鍵を用いて復号し、このように復号した得たデータを出力手段により外部に出力することができる。

【０１１５】これにより、データ受信装置は、多チャンネル及び大容量でデータの転送を通信衛星を利用したデータ伝送システムにおいて、スクランブル処理されて伝送されてくる信号を受信して、当該スクランブル処理されている信号をデスクランブルして得ることができるとともに、当該データ受信装置のみに宛てて配信された情報のみを意味のある情報として取り込むことができるようになる。

【０１１６】このデータ受信方法は、受信工程により衛星通信路を介して受信したスクランブル処理されている信号データを、デスクランブル工程によりデスクランブル処理を施し、ディジタルデータにして取り出し、そして、当該ディジタルデータから、データ取得工程により、所定のデータを取り出すことができる。そして、データ受信方法は、データ取得工程により取得した暗号化されているデータを、復号工程により暗号鍵を用いて復号し、このように復号した得たデータを出力工程により外部に出力することができる。

【０１１７】このデータ受信方法により、多チャンネル及び大容量でデータの転送を通信衛星を利用したデータ伝送システムにおいて、スクランブル処理されて伝送されてくる信号を受信して、当該スクランブル処理されている信号をデスクランブルして得ることができるとともに、当該データ受信装置のみに宛てて配信された情報のみを意味のある情報として取り込むことができるようになる。

【０１１８】また、本発明に係るデータ送信方法は、データ暗号化工程により、衛星通信路を介して配信するデータを暗号鍵を用いて暗号化処理するとともに、当該暗号化したデータの配信先情報を付加し、スクランブル処理工程により、当該データ及び情報に、映像音声情報の

23

スクランブルに使用されるスクランブル処理を施し、データ伝送工程により、このスクランブル処理されたデータを上記衛星通信路上に伝送することができる。

【０１１９】このデータ送信方法により、データが配信されるデータ受信側では、スクランブル処理されて伝送されてくる信号から暗号化されている情報を上記宛先情報に基づいて取り出し、当該取り出した暗号化されているデータを暗号鍵により復号することができる。これにより、このデータ伝送方法は、多チャンネル及び大容量でデータの転送を通信衛星を利用したデータ伝送システムにおいて、スクランブル処理されて伝送されてくる信号を受信して、当該スクランブル処理されている信号をデスクランブルして得ることができるとともに、所定のデータ受信装置のみに宛てて配信された情報のみを意味のある情報として取り込むことを可能にする。

【図面の簡単な説明】

【図１】本発明の実施の形態とされるデータ受信装置を備えるデータ送信システムの構成を示す図である。

【図２】上記データ受信装置の構成を示すブロック回路図である。

24

【図３】上記データ送信システムにおいて、配信の対象とされるデータに施す暗号化処理及びスクランブル処理の説明のために用いた図である。

【図４】上記配信の対象とされるデータがＩＰパケットに格納された場合に、当該ＩＰパケットに付加されるＩＰヘッダを示す図である。

【図５】上記ＩＰパケットがＭＡＣフレーム化された場合に、上記ＩＰヘッダの情報を格納するＭＡＣヘッダを示す図である。

【図６】上記データ受信装置のさらに詳しい構成を示すブロック回路図である。

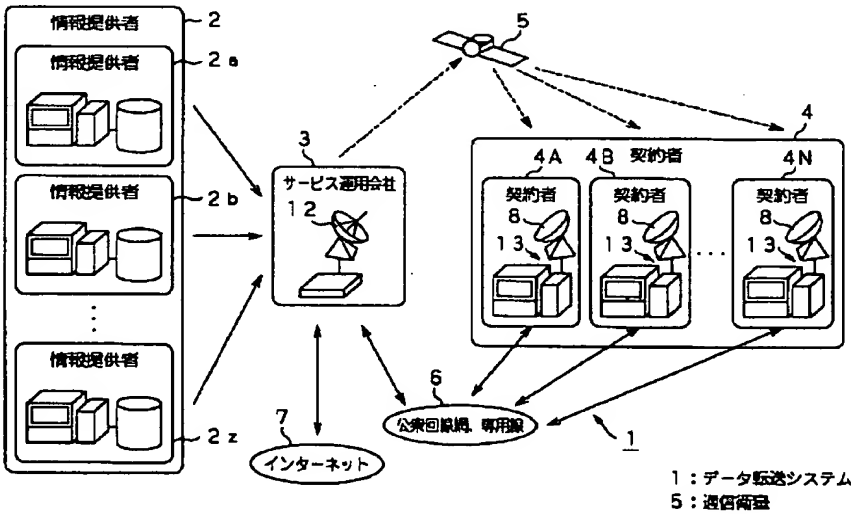
【図７】上記データ送信システムにおいて、配信されてくるデータに施すデスクアンブル処理及び復号化処理の説明のために用いた図である。

【図８】上記データ受信装置の変形例を示すブロック回路図である。

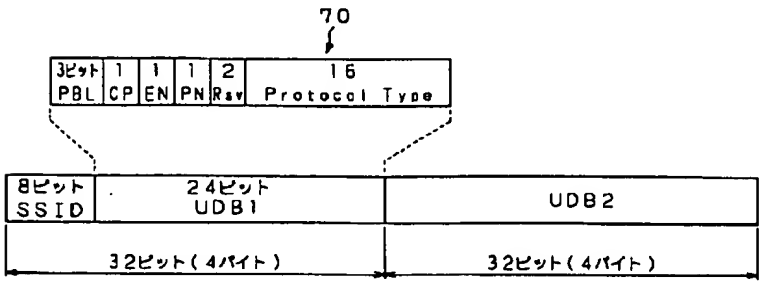
【符号の説明】

１　データ伝送システム、３０　受信アンテナ、３２　衛星データ取り込み装置、３３　データ復号装置、３５　受信データ出力Ｉ／Ｆ装置、３８　データ入力装置

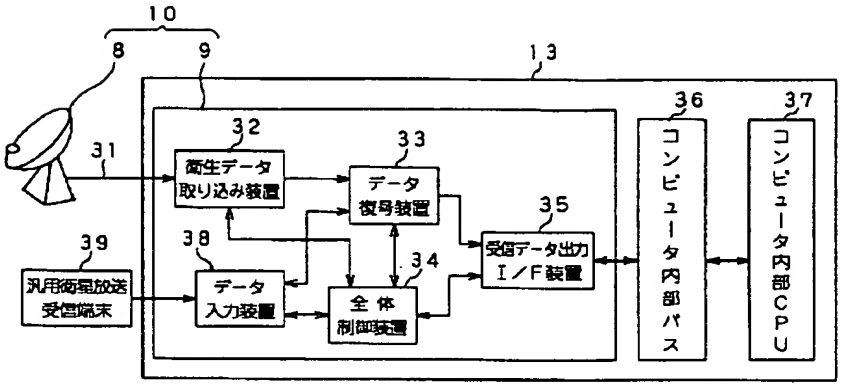
【図１】



【図５】

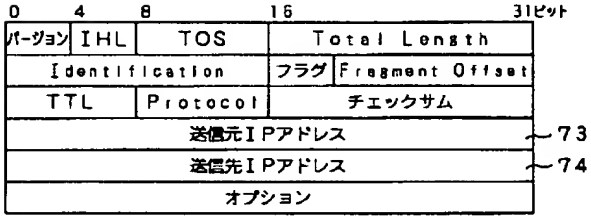


【図２】

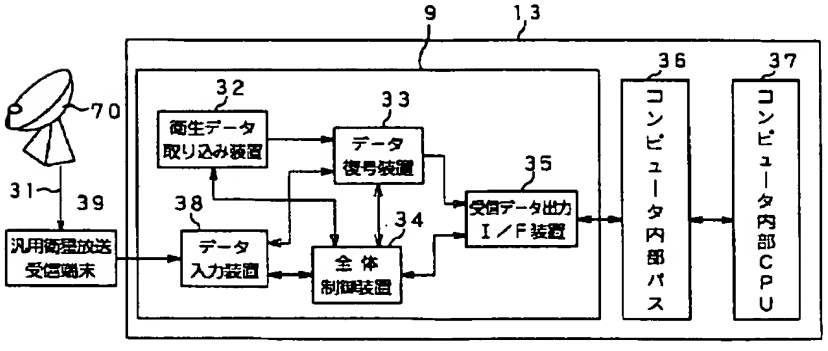


10：データ受信装置
13：コンピュータ
31：同軸ケーブル

【図４】

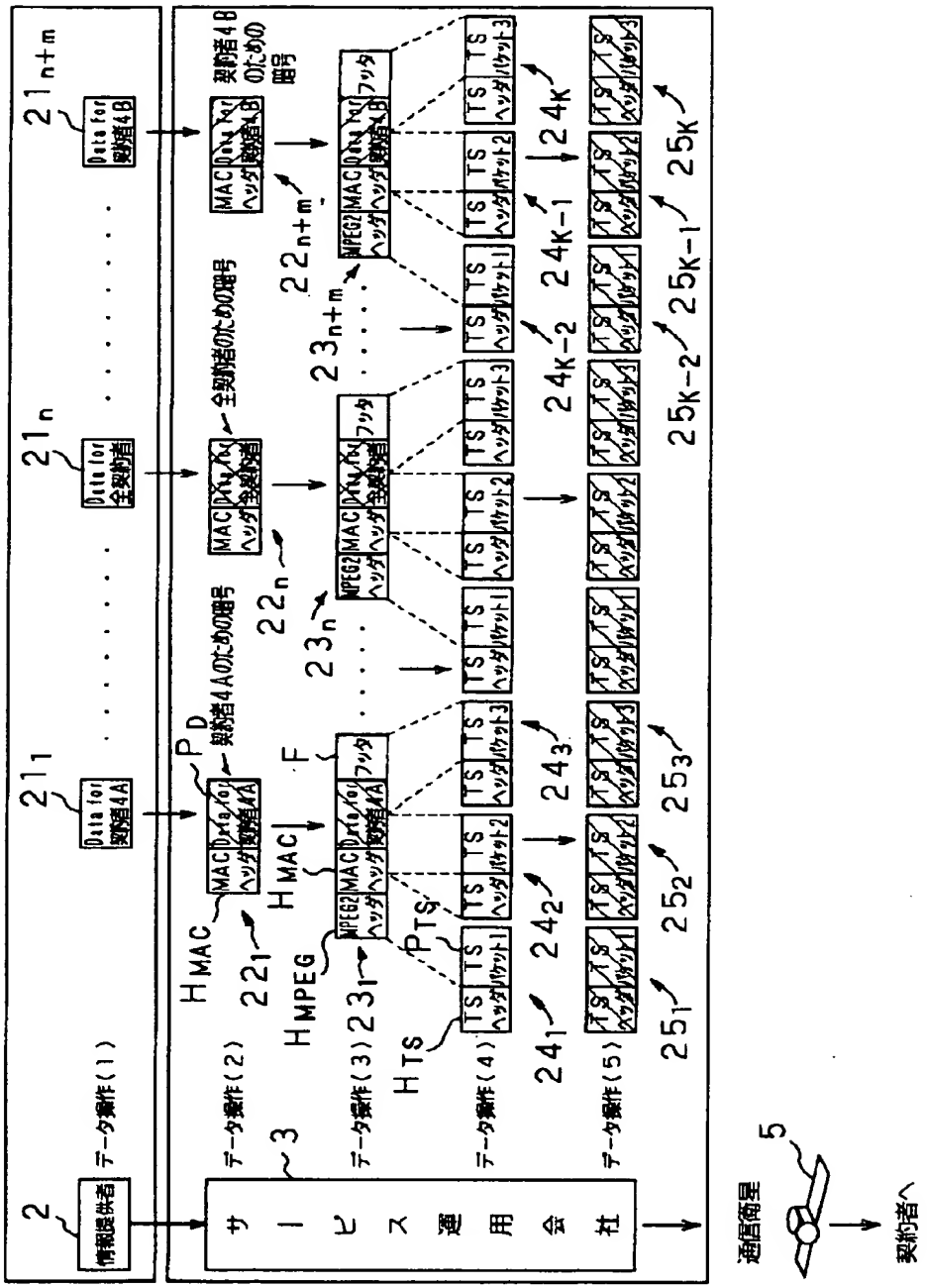


【図８】

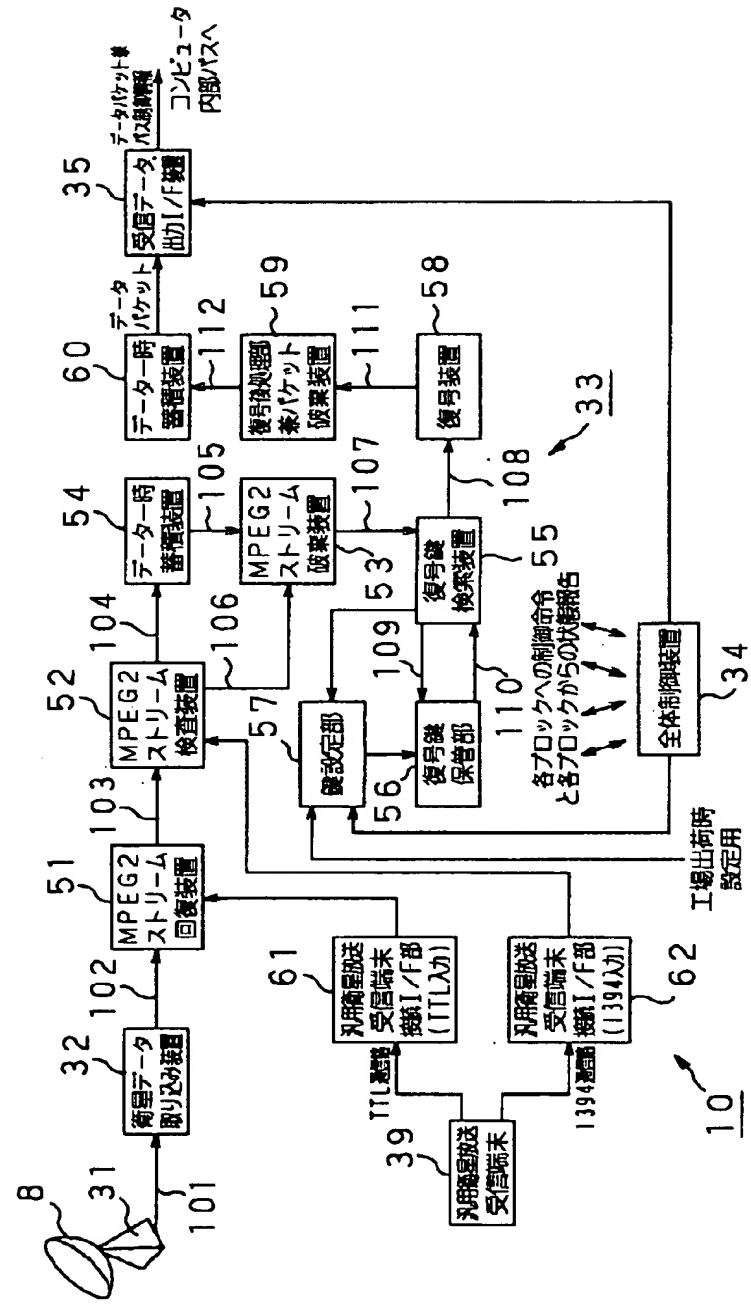


13：コンピュータ
31：同軸ケーブル

【図３】

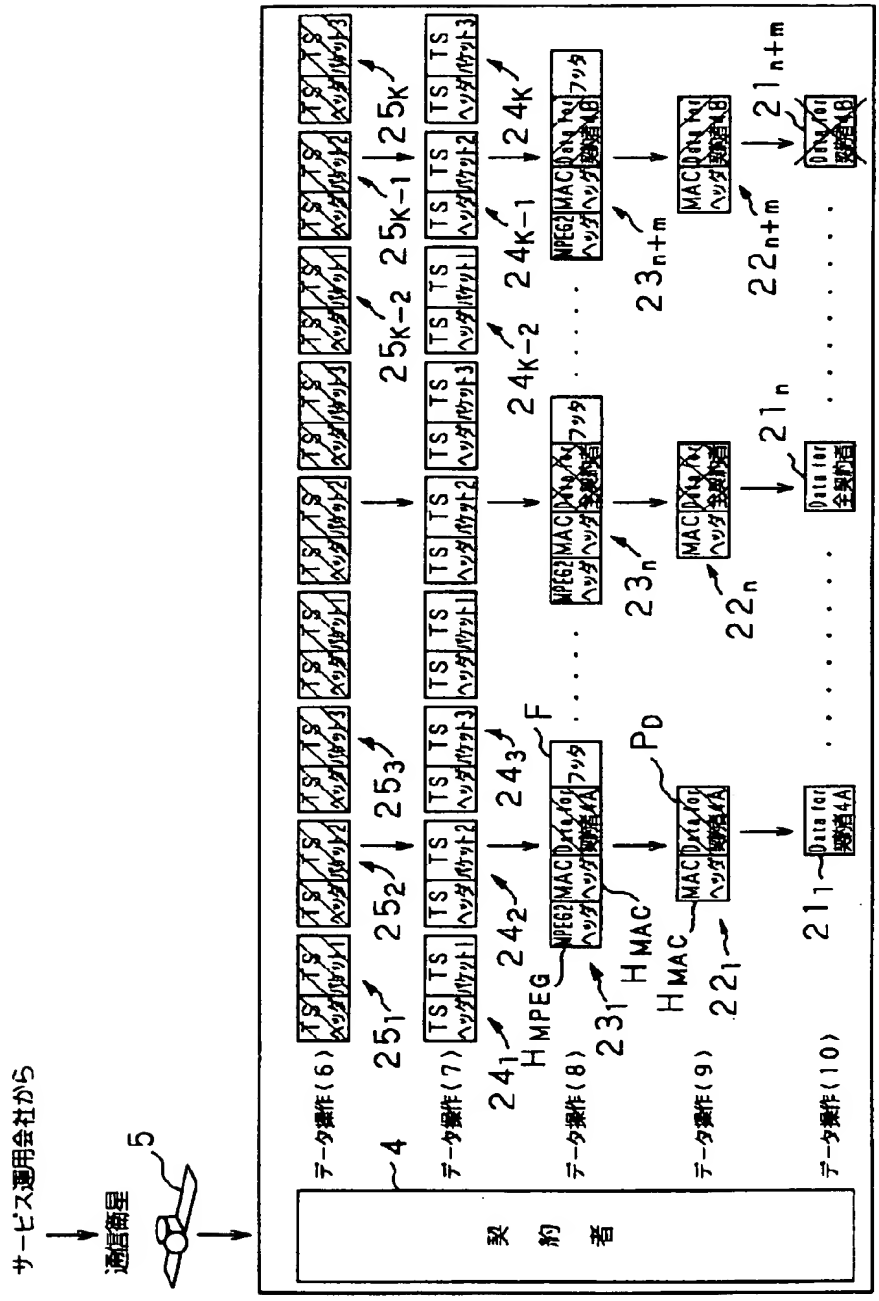

2
情報提供者
データ操作(1)
サービス運用会社
データ操作(2)
データ操作(3)
データ操作(4)
データ操作(5)
3
Data for 契約者A
Data for 全契約者
Data for 契約者B
21_1
21_n
21_{n+m}
P_D
H_{MAC}
H_{MPEG}
H_{TS}
P_{TS}
F
契約者Aのための暗号
全契約者のための暗号
契約者Bのための暗号
MAC ヘッダ 契約者A
MAC ヘッダ 全契約者
MAC ヘッダ 契約者B
MPEG2 ヘッダ
フッタ
TS ヘッダ
パケット1
パケット2
パケット3
22_1
22_n
22_{n+m}
23_1
23_n
23_{n+m}
24_1
24_2
24_3
24_{K-2}
24_{K-1}
24_K
25_1
25_2
25_3
25_{K-2}
25_{K-1}
25_K
通信衛星
5
契約者へ

【図6】



8：受信アンテナ
10：データ受信装置
101：IF受信データ
102：TSパケット
103：MPEG2ストリーム
104：MPEG2ストリーム
105：MPEG2ストリーム
106：MPEG2ストリーム
107：MPEG2ストリーム
108：復号鍵暗号データパケット
109：復号鍵要求命令
110：復号鍵
111：復号後データパケット
112：データパケット

【図７】


サービス運用会社から
通信衛星
5
4
契約者
データ業作(6)
データ業作(7)
データ業作(8)
データ業作(9)
データ業作(10)
25_1
25_2
25_3
25_{K-2}
25_{K-1}
25_K
24_1
24_2
24_3
24_{K-2}
24_{K-1}
24_K
23_1
23_n
23_{n+m}
22_1
22_n
22_{n+m}
21_1
21_n
21_{n+m}
H_{MPEG}
H_{MAC}
H_{MAC}
F
P_D
TS ヘッダ
TS パケット
MPEG2 ヘッダ
MAC ヘッダ
フッタ
Data for 受信者A